CHAPTER I.

The Hems and Haws Being Over, Let's Plunge Right In.

Getting Your Terms Straight

Although this little book is intended only to afford you some amusement for leisure moments, there is no reason why we shouldn't be accurate, so let's get one thing straight right off. We are not going to talk about "codes" in this book in the promiscuous manner so commonly heard with that term. If there is one thing that will give you away when talking with those who know their business in this field more quickly than anything else it is the mistake of calling a cryptogram a code message when it is really a cipher message, or vice versa. It's about as bad as if you were chinning with a radio shark and called a certain type of hook-up a "whizzadyne" whereas it most obviously was a "bloopoflex". Your reputation would be ruined instantly.

And if there's anything in the universe that makes me see red, it is for someone to talk about "deciphering codes". When an expert calls a cryptogram a code message (note that I say cryptogram and not cryptograph:--a cryptograph is a machine or a device that writes or assists in preparing cryptograms mechanically), he means that the cryptogram was prepared by the use of a book something like a dictionary. This book may, in fact, be a dictionary pure and simple, with

the words numbered, or indicated in some systematic manner, or it may be a specially printed book called a code book, or simply a code.*

---

* To my horror I discover that a certain unabridged dictionary (which shall remain nameless) speaks of a "cipher code"! Beware of such monstrosities.

The word code comes from the Latin codex, which means literally the stem of a tree. Hence any system of principles or rules is a codex or code; thus arises the definition in Webster's International Dictionary for the kind of code we are discussing: "a system of words or other symbols arbitrarily used to represent words." A good code book contains not only the most frequently used words, but also the most common phrases, or even sentences; and each word, phrase, or sentence that is listed separately is given a combination of letters or figures which can then be used to represent it. Then to convert a message into a cryptogram by means of this code book one merely replaces the words and phrases of the message by the equivalent code groups given by the book. The most usual form of code group today is a five-letter artificial "word", such as OMMFU or TAXIP.

By Their Codes Ye Shall Know Them

For example, by utilizing a small code book on my desk as I write, I can send the message "Referring to my telegram of the second of this month, why were instructions not given?" in two code words: RYNVO FLIRP. Here the first code group, RYNVO, represents the phrase "Referring to my telegram of the second of this month;" the second code group, FLIRP, represents the phrase "why were instructions not given?" There is usually no relation between the English words and phrases and the code groups that represent them.

There is really no reason why you should live another day without seeing exactly what a code book looks like. Anyone can walk into a

telegraph office and ask for the Western Union ~~or Postal Telegraph~~ Pocket Code. ~~(But don't ask for~~ the Western Union code book in a ~~Postal Telegraph office, or vice versa. That is, unless you want to be thrown out).~~ Just say that you have to send a cable message to your Great Aunt Mehitabel in Timbuctoo and that you want to borrow their code book, so that you can say it in as few words as possible. That's what the cable company had the code book made for--to be helpful to their customers. And then when you've read the code book through, so that you are very, very sure that in the future you will be perfectly certain to recognize the species, why you can just slip out when no one's looking.

And now let's hear no more of this business of calling a cryptogram "a code". It may be a code message; or it may be a cipher message; but once and for all, it is not "a code". So that's that.

Business men use codes mainly for one purpose: to cut down the cost of telegraphing or cabling. In the example given above, 15 words totalling 70 letters were transformed into two words totalling but 10 letters; and if the message were going by radio, telegraph or cable, the 10 letters are counted and charged for as two words. Of course a business man is sometimes interested in secrecy, too, and in that case he does not use ordinary codes that can be purchased in book shops, but has a code book specially prepared for his use. If, however, he uses an ordinary code book purchasable by anybody with the price, he usually plans to do something to the code message to make it unintelligible to a person who may have a copy of the code book but for whom the message is not intended. There's a lot more to this subject of code, but we've given enough now for our purpose, which was to prepare you to see how it differs from cipher.

Twin Brothers Economy and Secrecy

Cipher

The

Romantic

Child of

Cryptography

Just to point the moral once more:--in code you are dealing with units which are composed of syllables, words, phrases, or even sentences. In ciphers we usually deal with the individual letters of the message. We do something to the separate letters as units, and rarely if ever, treat entire words or phrases as units. There is always a definite relation of one sort or another between the letters being enciphered and the cipher letters that represent them.

There are thousands of ways of converting an unintelligible message into a cipher, but they can all be boiled down to two and only two basically different ones. That makes it look much easier, doesn't it? Let's see what these two fundamental ways are. I think I can show you in a jiffy by using a short sentence as an illustrative example: "Sympathizers being rounded up here." Remember I said that in ciphers we deal with individual letters, so let's start right in with the letters of the first word: S-Y-M-P-A-T-H-I-Z-E-R-S.

Miss

Transposition

Merely

Turned

Her

Clothes

Around

Now there are only two things I can do to that word to change it from a well-known friend into a perfect stranger. I can seize the word by the scruff of the neck, give it a good shaking, and make it look like a respectable town in the land of the Never-Never: PRZYMIHATSES. That's what is called transposition, because we have merely rearranged or transposed the letters from their original arrangement or order. Of course, I can treat the message as a whole by giving the entire business a good shaking, and get this out of it:

P Z E O D R Y H S G D H A E I U U E M I B R E E S T R N N P

It would still be transposition, because all the original letters are there--I've merely rearranged them. Sometime later I'll show you how to get them back again in their correct order even if you don't know what method was used to mix them up.

Miss Substitution Has Changed Into New Clothes

Now the only other thing I can do to the letters of the message is to replace them by other letters, or by symbols, figures, dancing men, or what not. For example, I can take this sentence "Sympathizers being rounded up here." and replace each letter by the one that follows it in the ordinary alphabet, and my, but doesn't it look like gibberish!

TZNQBUIJAFST CFJOH SPVOEFE VQ IFSF

That's what is called substitution. As I said before, I can replace the letters by symbols, figures, dancing men, and so on, so that I might get something like this out of the message:

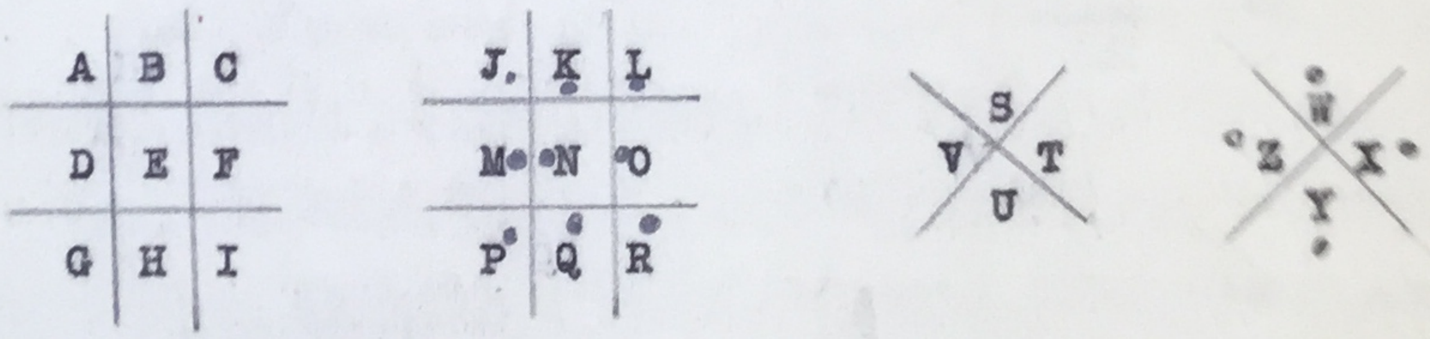
$ 3 / * 4 7 Z 8 K ? ; $ Q ? 8 X . ; % P X @ ? @ P * Z ? ; ?

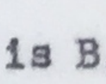
Or:

It is still substitution. Cryptograms like the last ones aren't so popular as they once were because you can't send them by telegraph. Anyhow, their peculiar appearance, far from adding an air of mystery to them--to the expert--really makes it easier for him because it's almost invariably a sign that the cryptogram was prepared by a person who doesn't know anything about cryptography, usually a child or the purest neophyte, and hence oughtn't to be hard to unravel.

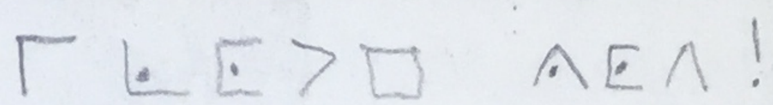
Job (who's he?) And The Boy Next Door Used This One

Here's one type that is "invented" daily, although it is so old that I'm sure Adam used it to send mash notes to Eve:

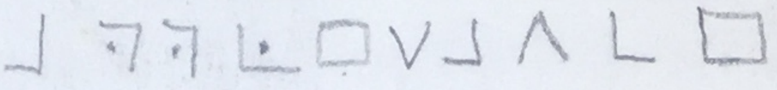


The various angles in these diagrams can be used to indicate the letters. Thus  is A,  is B,  is J,  is U,  is W, ...

See for yourself. This is probably what Adam said to Eve:

Adam: 

And this is undoubtedly how she replied:

Eve: 

Of course, one can put the letters in the diagrams in an arrangement different from the ones I've shown, but the principle is the same, and later on you will see how easy such cases are to solve. Anyhow, one thing about this type and the one with the dancing figures and the punctuation signs is that they show on their face that they are substitution ciphers to begin with. Away then with these simpletons, and let's go back to the real kind--those that consist of letters and letters alone.

And it is just as well to add for your information that while a telegraph or cable company will accept a message composed of groups that contain mixtures of letters and figures you'd have to pay for it, and how! For example, whereas the group KOBOL would be counted as only one word, the group K7B4L would be counted as five words. That's the rule, made by international convention, signed by umpsteen countries all over the globe; so there is nothing, I think you will agree, that you can do about that. Hence don't go "inventing" any ciphers which produce such mixtures of symbols, letters, figures, or what-have-you.

Look To The Purse Strings

There are hundreds of ways of producing transposition ciphers, and thousands of ways of producing substitution ciphers, but you need only one piece of information to be able to tell almost invariably whether a given cryptogram belongs to the transposition class or to the substitution class. This information may seem a bit complicated at first, but it really isn't at all. What's more, it's interesting for its own sake, and you've probably never thought about it before.

Sisters Don't Always Look Alike

Wherein We Learn A Thing Or Two About The Tools Of Language

Have you ever wondered about these little black marks that you are looking at and which carry to you some story which I hope will be worth the sum you spent to obtain it? They are parts of the white man's noblest and most remarkable invention--the alphabet. You're really in luck to have it and to be able to use it, because there are several hundred million human beings that haven't it, and couldn't use it if they had--like the great mass of the Chinese, for example. Our alphabet has had a long and interesting history, but we don't need to go into that. I just want to mention two or three things about our particular alphabet, because they will help us understand ciphers a bit better.

Now I wouldn't be a bit surprised to learn that there are some persons reading this book who if suddenly awakened from a sound sleep would not be able to recite the alphabet, so here it is:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

It is composed of 26 letters and their order is fixed. I couldn't for the life of me tell you why A comes first, B second, and so on, nor can anybody else tell you,--and don't let them kid you into thinking they can, either. Of course it's easy to say that A comes first because in the alphabet which is the papa of them all (there are many alphabets beside our own) A comes first. But then that's no answer. I suppose at one time the letters had a great argument among themselves as to which should come first, which second, and so on, but at present an armistice is in force, and X Y Z seem to be resigned to their fate of being in the class of also-rans and occupying positions at the tail end. If I were appointed to act as final arbitrator at the peace conference between the warring letters what I would do would be to send

my intelligence agents out and tell them to find out which ones deserved to be placed at the head of the class on the basis of the amount of work each one did. My agents would snoop around on gum shoes, spend a lot of my money and when they got tired would sit down and make an actual count of letters in a large amount of ordinary telegrams, and then, like all that species called efficiency engineers, they'd probably turn in a report like this:

"With reference to the efficiency tests of the activities of the letters of the English alphabet, as used in ordinary telegrams, we beg leave to present the results of our investigation in the form of a chart shown herewith as Figure 1.

This chart, which we call a <u>frequency table</u>, was made by counting the letters that occurred in various kinds of telegrams, totalling 100,000 letters. We call your attention respectfully to the fact that certain letters which are putting forth claims for preference are in reality slackers of the worst kind, whereas certain other letters which have been satisfied to do more than their fair share of the work to be done are now occupying more or less insignificant positions in the list. On the basis of our investigation if we were to arrange the letters in the order of their importance, judged by the work they do, they would appear as follows:

E T O A N I R S H D L U C M P F Y W G B V K J X Z Q

You will also note from Figure 1 that ten letters, E, T, O, A, N, I, R, S, H, and D, do almost 75% of the work; the four vowels, A, E, I, and O, doing about 35% of it; the six consonants, D, H, N, R, S, and T, doing a bit more, 40%. This leaves 16 letters to do the rest, that is, 25% of the work.

The hardest workers are E, T, O, A, and N, and the worst slackers are J, K, Q, X, and Z.

Attached hereto is our bill for services rendered.

Very truly yours,

F. FISH ENSEE."

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Figure 1.--Frequency table for normal English text.

Now if you have digested this report you will be able to follow me in the simple reasoning by means of which you can tell a transposition cipher from a substitution cipher.

Do you remember what I said about a transposition cipher? In that type the letters of the original are merely shifted around. Therefore, the proportions given in the report of our efficiency experts should still hold. That is, the vowels A, E, I, and O should form about 35% of the total, the hard working consonants D, H, N, R, S, and T should form about 40%, and the slackers J, K, Q, X, and Z should be up to their usual tricks, that is, AWOL most of the time.

Now we can argue backwards something like this: If in a given cryptogram we count the letters of each kind and find that the vowels A, E, I, and O form approximately 35% of the total, the hardworking consonants D, H, N, R, S, and T about 40%, with the slackers J, K, Q,

The
Thee
And
Thou
Of
Ciphers

X, and Z mostly playing hookey, then we can almost be sure that the cryptogram is a transposition cipher because the letters are present in the proper proportions required for intelligible English.

Of course you must bear in mind that the efficiency experts made their investigation upon a very large amount of text, and their results are true only in the long run, that is, in a large amount of text, giving a high batting average. In a small amount of text the proportions given almost never run absolutely true to form, and we should allow a 5% leeway above or below the average.

But if the count shows proportions considerably different from the normal, even allowing a leeway of 5% above or below, then you can be sure that the cryptogram is a substitution cipher. For instance, if the vowels A, E, I, and O totalled roughly 16%; the high-frequency consonants D, H, N, R, S, and T, approximately 12%; and the low-frequency consonants J, K, Q, X, and Z, about 42%, then the cryptogram is certainly a substitution cipher. And positively no ifs, ands, or buts about it.

CHAPTER II.

Getting Down to Business

There's nothing like a concrete case to clear up a point, so let's try a sample.

Example 1.

PDAWJ WHUPE YWHLK SANOD KQHZJ KPXAY KJOKQ JZAZS

EPDOE ILHAE JCAJQ EPUTB KNSDE HAPDA WJWHU OPEOJ

AYAOO WNEHU EJCAJ EKQOP DAEJC AJEKQ OIWJE OKBPA

JEJYW LWXHA KBJWW HUOEO

We Must Look Professional At All Costs

You were surprised, no doubt, when you first got the impression of the regular groups of five letters. Well, you may just get it out of your head right now that the problems in this book are going to be so foolish as to give you half the answer at the start by showing you the original word lengths. Where ciphers are used for serious purposes, and by people who know their business, the final cryptograms show only five-letter groups (or sometimes five-figure groups). There are two reasons for this. In the first place, it makes it harder for some busybody (like you're trying to learn to be) to read the message. In the second place, where the message is to be sent by land telegraph, they charge you for it at the rate of five letters per word, and although you can have them send it in any arrangement of word length you please, it insures accuracy to have the stuff broken up into regular groups of fives. The telegraph operators can handle it much better

that way. So from now on, all the cryptograms you are going to handle will be in the form of five-letter groups.

This is as good a place as any to tell you that in this country if you send a telegram consisting entirely of figures, no matter how you group them, each figure counts as a whole word. A group like 79235 costs you five words. That's enough to make you understand why business men don't use figure telegrams very much.

Well, to get back to Example 1. The first thing to do is to make a frequency table, like this:

Figure 2.

Hot

Stuff!

A - 15	D - 6	J - 16	Total number of letters = 140
E - 15	H - 9	K - 10	
I - 2	N - 3	Q - 5	A E I O = 43 = 31%
O - 11	R - 0	X - 2	D H N R S T = 22 = 15%
43	S - 3	Z - 3	J K Q X Z = 36 = 26%
	T - 1	36	
	22		

So far as the vowels are concerned, a total of 31% is plenty high enough to make you think it might be a transposition, but if you went ahead on that idea without looking any further you'd soon find yourself at the end of the proverbial blind alley. Take a look at the number of high-frequency consonants, D, H, N, R, S, and T--only 15% --and that of the slackers, J, K, Q, X, and Z, 26%. When those boys begin to get very busy and stir up a lot of dust you can be sure the dust is for your own eyes. No, indeed! You won't be fooled so easily --it's a substitution cipher, without a doubt.

Mercy! Haven't We Finished With That Yet?

Well, we won't try right away to solve that one, though it is simple enough. What we want to do now is to get straight on the difference between Transposition and Substitution Ciphers. Take a look at the next cryptogram. The English of it is exactly the same as that for the preceding message, but notice the percentages and frequency table.

Example 2.

TCOOI NOAEI HSNOH AUNTG RNCNE MIFEL LFHEW AECIA NAAPD

OSNHL SENNC NNONU IUIYS NGIAA AWONM ILSAI ESPLL ETDPT

ETRON OAYYR BELYT IIUIF BSTSE DEXHS LSOTL IIHCW IFENY

TUEES

Here's the frequency table:

Figure 3.

Pretty Snigget!

Total number of letters = 140

A - 11	D - 3	J - 0
E - 15	H - 6	K - 0
I - 15	N - 16	Q - 0
O - 10	R - 3	X - 1
51 = 38%	S - 11	Z - 0
	T - 9	1 = ½%
	48 = 34%	

Compare these percentages with those given on page 0 for average English text, and I think you'll agree that it doesn't require much deliberation to decide that we are dealing with a transposition cipher.

There's just one more thing I want you to notice about the normal frequency table (page 0) while we're still on the subject. If you

will hold the table up in front of you and take note of where the most prominent high spots and low spots fall, you will see that they go something like this:

Figure 4.

Over

The

Hurdles

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Keep this in mind, if you can, and if you can't, it will be here when you need it later. That is the typical shape of the frequency table for ordinary English text--and for a transposition cipher, too, because in that type of cryptogram all the letters of the original English are still there--they have only been shaken up a bit and disarranged.

Now let us go back and solve that first example on page , which we saw clearly was a substitution cipher.

Now I'm going to let you in on a little trick that will interest and help you lots of times. First we'll do the trick and then we'll explain it.

Write the first three or four groups of the cipher at the top of a sheet of paper and draw a line under them. Like this:

Listen,

All Ye!

This Is

Good

P D A W J W H U P E Y W H L K

The first letter of the message is P. Under it write down in a column, equally spaced, the letters that follow P in the ordinary alphabet, and when you get to Z go right on with A, B, C, and so on until you get to P again. Thus:

P	D	A	W	J	W	H	U	P	E	Y	W	H	L	K
Q														
R														
S														
T														
U														
V														
W														
X														
Y														
Z														
A														
B														
C														
D														
E														
F														
G														
H														
I														
J														
K														
L														
M														
N														
O														

Figure 5.

Then do the same thing under the second letter, D, only of course, you write E, F, G, and so on. Then under the third letter, A, continue with B, C, D, and so on. Do this stunt under each letter, and this is what you'll get:

P	D	A	W	J	W	H	U	P	E	Y	W	H	L	K
Q	E	B	X	K	X	I	V	Q	F	Z	X	I	M	L
R	F	C	Y	L	Y	J	W	R	G	A	Y	J	N	M
S	G	D	Z	M	Z	K	X	S	H	B	Z	K	O	N
T	H	E	A	N	A	L	Y	T	I	C	A	L	P	O
U	I	F	B	O	B	M	Z	U	J	D	B	M	Q	P
V	J	G	C	P	C	N	A	V	K	E	C	N	R	Q
W	K	H	D	Q	D	O	B	W	L	F	D	O	S	R
X	L	I	E	R	E	P	C	X	M	G	E	P	T	S
Y	M	J	F	S	F	Q	D	Y	N	H	F	Q	U	T
Z	N	K	G	T	G	R	E	Z	O	I	G	R	V	U
A	O	L	H	U	H	S	F	A	P	J	H	S	W	V
B	P	M	I	V	I	T	G	B	Q	K	I	T	X	W
C	Q	N	J	W	J	U	H	C	R	L	J	U	Y	X
D	R	O	K	X	K	V	I	D	S	M	K	V	Z	Y
E	S	P	L	Y	L	W	J	E	T	N	L	W	A	Z
F	T	Q	M	Z	M	X	K	F	U	O	M	X	B	A
G	U	R	N	A	N	Y	L	G	V	P	N	Y	C	B
H	V	S	O	B	O	Z	M	H	W	Q	O	Z	D	C
I	W	T	P	C	P	A	N	I	X	R	P	A	E	D
J	X	U	Q	D	Q	B	O	J	Y	S	Q	B	F	E
K	Y	V	R	E	R	C	P	K	Z	T	R	C	G	F
L	Z	W	S	F	S	D	Q	L	A	U	S	D	H	G
M	A	X	T	G	T	E	R	M	B	V	T	E	I	H
N	B	Y	U	H	U	F	S	N	C	W	U	F	J	I
O	C	Z	V	I	V	G	T	O	D	X	V	G	K	J

Figure 6.

Now look carefully at each horizontal line of this diagram. What do you see on the fourth line under the cipher text? Eureka! Why it's good English. THE ANALYTICAL PO.... How on earth did that happen?

Oh, Dear, Nothing New Under The Sun

Well, let's go back a few thousand years. No, this particular method of solution isn't quite that old, but the method of preparing the cipher is. In fact Julius Caesar used it and Julius probably stole the idea from Noah, or some other old bird way back, because the old Hebrews were wise to it.

Suppose you write the alphabet down, and then under it write another alphabet, only begin A under B of the upper line. Like this:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

To complete the business we ought to add Z just in front of the A on the second line, or else add A just after Z on the first line, or both if we wish:

English - A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
Cipher - Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

This Term Will Be Worth A Lot To You

This is now what's called a cipher alphabet--and by using it we can write in cipher. Consider the upper line as the one from which to take the English letters, the lower as the one from which to take the cipher letter. For example, letter A of the plain English text equals Z in the cryptogram; letter B equals A in the cryptogram, and so on. Thus, by means of this alphabet the word CIPHER can be put into strange form as follows:

C I P H E R
B H O G D Q

Now you can imagine the upper line of letters as being fixed in position, and the lower line as being on a strip of paper which you can move to the right or left as you please. Then it's clear that

you can make a set of 25 different cipher alphabets by sliding the lower strip hither and yon, and have a good time with them. You could write the same English message in 25 different cipher forms, no two being alike in a single letter. For example, if you slide the lower line one more space to the right--like this:

English - A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Cipher - Y Z A B C D E F G H I J K L M N O P Q R S T U V W X

and write the word CIPHER in cryptographic form again, you get AGNFCP, which bears no resemblance to the previous form, BHOGDQ. You don't have to use just plain strips of paper. If you are inclined to make something fancy, you can fix up a fine little cipher device by making two concentrically* revolving disks like this:

Gracious! What Have We Here?

- -

* Don't be frightened by this word: it merely means both disks are pivoted con (with) centric (center) to each other.

- -

Figure 7.

If you are inclined toward fancy work, but are not industrious enough to make one of these handy little devices yourself, fill out the blank at the end of this book and send for one (with a consideration).

Now if you and Dick Roe decide to communicate in cipher, and each of you had a disk like this, all you would have to agree upon in order to send messages in cipher would be where to set the inside disk at the start.

For example, suppose you agreed to set them so that A on the inside wheel is opposite E of the outside wheel, that is, so that E of the plain text is represented by A of the cipher text, or, as we shall hereafter indicate letters, so that E_p equals A_c. (E(plain) = A(cipher). This will avoid all possible confusion, and will save lots of words.)

Boy, Is This Neat!

The setting of the disks is shown in Figure 8.

Figure 8.

If you enciphered the words THE ANALYTICAL you would get the following:

English - T H E A N A L Y T I C A L
Cipher - P D A W J W H U P E Y W H

which, when put in five-letter groups, would read as follows:

PDAWJ WHUPE YWH..

Isn't that how our first cipher example started out? Yes, the secret is out. But shucks, it can't be much of a cipher, because we solved it in a hurry. Almost mechanically. All we did was to con-

tinue the ordinary alphabet under the cipher letters and the answer stuck right out as plain as the nose on your face. Why was that? Supposing that the inner disk is set against the outer one at some other point, would it make any difference at all so far as the simplicity of this solution goes? Not at all. If you don't believe me, try it and convince yourself. Well, what's the reason for all this?

Look at it in this way. Let's suppose that you have the pair of concentric disks I spoke of, and the message beginning PDAWJ WHUPE etc. You don't know anything about this little method of solution I've just shown you, but, being anxious to solve the message you decide to try out every possible position of the two disks. Suppose you set the inner disk so that its A is opposite B of the outer (A_c equals B_p), and then you try to decipher the message. This is what you'd get:

Trials And Tribulations

Cipher - PDAWJ WHUPE
"English" - QEBXK XIVQF

That doesn't even look like good Russian, (that's why I put the word "English" in quotation marks in the line above) so you advance the inside disk one more letter, making A_c equal C_p, and try again. Here it is:

Cipher - PDAWJ WHUPE
"English" - RFCYL YJWRG

That's just as bad, so you try once more with A_c equaling D_p.

Again:

Cipher - PDAWJ WHUPE
"English" - SGDZM ZKXSH

Dear, dear me! We're getting nowhere fast. But once more, with A_c equaling E_p:

Cipher - PDAWJ WHUPE
"English" - THEAN ALYTI

Here we are. On the fourth trial we got it. But now just take a good look at the successive results for English given by the four trials. Put them under each other.

Cipher -	PDAWJ	WHUPE
1st Trial $A_c = B_p$ -	QEBXK	XIVQF
2nd Trial $A_c = C_p$ -	RFCYL	YJWRG
3rd Trial $A_c = D_p$ -	SGDZM	ZKXSH
4th Trial $A_c = E_p$ -	THEAN	ALYTI

Figure 9.

I think you can see what I'm driving at. The real English text came out on the fourth line because the inside disk had been advanced exactly four letters when the message was put into cipher. When you started to solve the message you didn't know that fact--that was the "secret". If it had been advanced eleven letters, why then in solving the message by our method the answer would have come out on the eleventh line, and so on. Each column in the little diagram above, Figure 6, is nothing but a complete alphabet beginning at a certain point, indicated by the cipher letter standing at its head. When you continue the alphabet under each letter it is the same as though you made trial after trial with the two sliding strips of alphabets, or with the revolving disks. Only the process I've shown you is much faster.

Whys And Wherefores

Suppose you had at hand a set of paper strips containing the normal English alphabet. Having some one flash that cipher message on you suddenly, all you'd have to do would be to set up those strips one against the other so that the first ten or fifteen letters of the message all appear on the same horizontal line, as was shown in Figure 6, and then search the horizontal lines of the resulting diagram for good English. Turn back to Figure 6 and look at it carefully once more. You will notice in this diagram that the strips should have double alphabets, that is, the alphabet should be repeated so that there will

be 52 letters on each strip. The reason is that only with a double alphabet sequence will there be 26 complete horizontal lines either above or below the cipher line.

You can easily make a set of these strips yourself, or you can get a fine set by filling out the blank at the end of this book. (Aways for a consideration, of course). You'll find them very useful.

CHAPTER III.

Get Set--Ready--Go!

Now then, for a practical test of what you have learned. Tackle this one:

Problem 1.

LNTAS PCLWA SLMPE ZCLDT ETDDZ XPETX PDNLW WPOLD FMDET EFETZ YLWAS
LMPET DZYPT YHSTN SESPP WPXPY ELCJZ CLWAS LMPET NDZFY ODDAP LVTYR
TYLMC ZLOYZ YEPNS YTNLW DPYDP LCPCP ACPDP YEPOM JNSLC LNEPC DZESP
CESLY ESZDP CPACP DPYET YRESP XTYES PYZCX LWZCZ COTYL CJLWA SLMPE

The Sense Zigzags

I suppose the first variation of this simple cipher that occurs to you right off is this: what if the key changes after each sentence, or in other words, what if the position of the inside disk is changed after each sentence? Well, supposing it is, what of it? Will it make the unraveling of such a cipher any more difficult? Not at all --that is, by the method I've shown you. The only thing that happens is that as soon as you get to the place where the key changes, the English will come out on a different line of the solving diagram (the one with the alphabets in columns) and will continue to come out on that line until the key changes once more. Try it on this one:

Problem 2.

BPMMV OTQAP TIVOC IOMQA EZQBB MVJGU MIVAW NIAMB WNBEM VBGAQ FAQUX
TMKPI ZIKBM ZAKIT TMLKW TTMKB QDMTG IVITX PIJMB ZAFMX XIDUF FQZXM
ZSGMS QEMDQ ARFTU EZMFG DQQEB ZEFKB PBIXK DRXDB CLOBU XJMIB FPTOF
QQBKY VJBXK PLCZL JMIBU ZEXOX ZQBOP BXZEO BMOBP BKQFK DXJLK LPVII
XYIBX KALKB PBKPB LCXTL OA

But suppose the key shifts with each word. To show you what I mean by that, suppose Mr. A and Mr. B agree to exchange cipher communications by means of the disks we have been using, and suppose that they agree beforehand that they will use the word SECRET as a key, changing the setting of the inside disk after each word they encipher according to the letters of the keyword selected. Let the message be: COME IMMEDIATELY. HAVE VERY IMPORTANT NEWS FOR YOU. Take your disk and set the inside one so that S (the first letter of the keyword SECRET) is under A of the outside series of letters ($A_p = S_c$). Then encipher the word COME. You will find it equals UGEW. The first word of the message having been enciphered, the key changes and the inside disk is moved so that $A_p = E_c$, to correspond with the second letter, E, of the keyword SECRET. The second word, IMMEDIATELY, is now to be enciphered, and comes out as MQQIHMEXIPC. Then the third word is enciphered with the key letter C, the third letter of the key ($A_p = C_c$), and so on. Check up on the following encipherment and make sure you understand the method:

More High Jinks

Example 3.

Key -	A_p=S_c	A_p=E_c	A_p=C_c	A_p=R_c	A_p=E_c	A_p=T_c	A_p=S_c	A_p=E_c
English -	COME	IMMEDIATELY	HAVE	VERY	IMPORTANT	NEWS	FOR	YOU
Cipher -	UGEW	MQQIHMEXIPC	JCXG	MVIP	MQTSVXERX	GXPL	XGJ	CSY

You'll notice that when the keyword has been used once, it is repeated, the word being used as many times as necessary to encipher the message. The message is divided up into five-letter groups, as usual:

UGEWM QQIHM EXIPC JCXGM VIPMQ TSVXE RXGXP LXGJC SY

Guess Again!

Notice that the same English letter is represented by different cipher letters, depending upon the position. For example, the letter E is represented by W, I, G, V and X. That makes it look pretty safe, doesn't it?

Figure 10

U G E W M	Q Q I H M	E X I P C	J C X G M
V H F X N	R R J I N	F Y J Q D	K D Y H N
W I G Y O	S S K J O	G Z K R E	L E Z I O
X J H Z P	T T L K P	H A L S F	M F A J P
Y K I A Q	U U M L Q	I B M T G	N G B K Q
Z L J B R	V V N M R	J C N U H	O H C L R
A M K C S	W W O N S	K D O V I	P I D M S
B N L D T	X X P O T	L E P W J	Q J E N T
C O M E U	Y Y Q P U	M F Q X K	R K F O U
D P N F V	Z Z R Q V	N G R Y L	S L G P V
E Q O G W	A A S R W	O H S Z M	T M H Q W
F R P H X	B B T S X	P I T A N	U N I R X
G S Q I Y	C C U T Y	Q J U B O	V O J S Y
H T R J Z	D D V U Z	R K V C P	W P K T Z
I U S K A	E E W V A	S L W D Q	X Q L U A
J V T L B	F F X W B	T M X E R	Y R M V B
K W U M C	G G Y X C	U N Y F S	Z S N W C
L X V N D	H H Z Y D	V O Z G T	A T O X D
M Y W O E	I I A Z E	W P A H U	B U P Y E
N Z X P F	J J B A F	X Q B I V	C V Q Z F
O A Y Q G	K K C B G	Y R C J W	D W R A G
P B Z R H	L L D C H	Z S D K X	E X S B H
Q C A S I	M M E D I	A T E L Y	F Y T C I
R D B T J	N N F E J	B U F M Z	G Z U D J
S E C U K	O O G F K	C V G N A	H A V E K
T F D V L	P P H G L	D W H O B	I B W F L

You're wondering, I suppose, why we set the key letter on the inside disk against A on the outside one. Well, you've got to have some understanding as to what letter you'll set the key letter against, and it seems easiest to remember that the value of A_p changes according to the successive key letters. Of course, you could agree to set the key letter against any other letter you please, but it won't make a bit of difference to us in solving such a cryptogram because we don't give one hoot about the key. We can solve it without the key altogether. Instead of the plain English all coming out on the same line, as was the case in Example 1 (and Problem 1, if you've solved it), or on three different lines, as was the case in Problem 2 (Don't tell me you haven't solved that cinch), the successive words of the English text will now come out on different lines. Let's take that Example 3 and solve the first four groups by our method of using the sliding strips.

Figure 10

Curiosity Won't Kill This Cat

Of course, if you're curious to know whether the correspondents are using a keyword in such a case, all you have to do is to take the first letter of each English word and its cipher equivalent, and then find what A_p equals. For example, having found that the first letter of the first word, COME, was represented by U ($C_p = U_c$), this means that the two disks were set so that C on the outside disk equalled U on the inside disk. Now set your two disks accordingly, and then see what A on the outside disk equals. S, doesn't it? Well then, when $C_p = U_c$, $A_p = S_c$ and hence the first letter of the keyword is S. Then take the first letter of the second English word, that is, the I of IMMEDIATELY, and its cipher equivalent M_c. When $I_p = M_c$, what does A_p equal? Set I on the outside disk to M on the inside. What does A on the outside equal? E, doesn't it? Then $A_p = E_c$, and hence the second letter of the keyword is E. Thus, the keyword begins with SE. I think you get the idea.

Try the next problem, and see if you can work out the key. I know you will get the English all right, but try your hand at finding the key.

Problem 3.

ETARV QITCR JAZJR FCHRX TCRTP ABVAS APFOQ SGGRR KYVME THODS PCSKL CPJLZ UFCPC ZWCPZ EKVCC ZXZSC VUPGR RCLBT HHPVT FTRPS IUTBK XZKJZ EKFAN JCXCI TAAXV XQATV YQCAP CRHQT O

I think that you have noticed that the cipher alphabets with which you have been dealing are made up of two series of letters--a series from which the plain English letter comes, and another series from which the cipher letter comes. For example, in each of the cipher alphabets that we have used as illustrations thus far the upper half is labeled "English" and the lower half is labeled "Cipher".

It is necessary, in case you have not already noticed it, to call your attention to the fact that both lines of letters in the cipher alphabets proceed in the same direction, which here happens to be from left to right. But suppose one of them runs in the opposite direction, like this:

Figure 11

English - A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Cipher - Z Y X W V U T S R Q P O N M L K J I H G F E D C B A

Reverse Gear

You could, of course, have the lower series of letters begin at any point, that is, with its A under any letter of the upper series, and in this way get a set of 26 cipher alphabets. Or, if you prefer working with concentric disks, all you need to do is to have the letters on one disk proceed in the same direction as the hands of a clock, while those on the other disk go counter-clockwise. Thus:

Figure 12.

I want to call your attention to a peculiar fact in connection with such cases. Whenever two alphabets are set against each other but run in opposite directions, the values all show reciprocity in pairs. By which is meantthat, in Figures 11 and 12, $A_p = Z_c$ and $A_c = Z_p$; $E_p = V_c$ and $V_p = E_c$, and so on.

Let us encipher a message with this disk and see what happens. We will take the same message as was used in Example 1, and set the disks at the same key letter as was used in that example, where A of the inside disk was set opposite E of the outside one ($A_c = E_p$).

Figure 13.

English - A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Cipher - E D C B A Z Y X W V U T S R Q P O N M L K J I H G F

Example 4.

THEAN ALYTI CALPO WERSH OULDN OTBEC ONFOU NDEDW ITHSI MPLEI
LXAER ETGLW CETPQ IANMX QKTBR QLDAC QRZQK RBABI WLXMW SPTAW

NGENU ITYXF ORWHI LETHE ANALY STISN ECESS ARILY INGEN IOUST
RYARK WLGHZ QNIXW TAIXA ERETG MLWMR ACAMM ENWTG WRYAR WQKML

HEING ENIOU SMANI SOFTE NINCA PABLE OFANA LYSIS
XAWRY ARWQK MSERW MQZLA RWRCE PEDTA QZERE TGMWM

Figure 14.

L	X	A	E	R	E	T	G	L	W
M	Y	B	F	S	F	U	H	M	X
N	Z	C	G	T	G	V	I	N	Y
O	A	D	H	U	H	W	J	O	Z
P	B	E	I	V	I	X	K	P	A
Q	C	F	J	W	J	Y	L	Q	B
R	D	G	K	X	K	Z	M	R	C
S	E	H	L	Y	L	A	N	S	D
T	F	I	M	Z	M	B	O	T	E
U	G	J	N	A	N	C	P	U	F
V	H	K	O	B	O	D	Q	V	G
W	I	L	P	C	P	E	R	W	H
X	J	M	Q	D	Q	F	S	X	I
Y	K	N	R	E	R	G	T	Y	J
Z	L	O	S	F	S	H	U	Z	K
A	M	P	T	G	T	I	V	A	L
B	N	Q	U	H	U	J	W	B	M
C	O	R	V	I	V	K	X	C	N
D	P	S	W	J	W	L	Y	D	O
E	Q	T	X	K	X	M	Z	E	P
F	R	U	Y	L	Y	N	A	F	Q
G	S	V	Z	M	Z	O	B	G	R
H	T	W	A	N	A	P	C	H	S
I	U	X	B	O	B	Q	D	I	T
J	V	Y	C	P	C	R	E	J	U
K	W	Z	D	Q	D	S	F	K	V

If you will compare the cipher text of this message with that of Example 1, you will see that they are entirely different. The question now is, how can such a cipher be solved? Can you use the vertical alphabet strip method? Well, let's try it. Set up the first ten letters on the strips, or examine this diagram on the left. You can't find a line beginning with THE AN... can you? It doesn't look as though our method will work here. What is wrong? I suppose the answer has already suggested itself to you. In the case of Example 1 we used a cipher alphabet in which both sequences of letters making up the cipher alphabet--the English series and the cipher series

--travelled in the same direction, whereas, in this example, the English series goes from left to right, and the cipher series goes in the reversed direction, that is, from right to left. Well, what shall we do?

Let us go through the following line of reasoning. Suppose we know only that the message was enciphered by a cipher alphabet in which both sequences were the ordinary alphabet but they ran in opposite direction (they are usually called "reversed alphabets"). We can take our reversed alphabet disk, or if you prefer, two strips of alphabets, one having the alphabet sequence going from left to right, the other from right to left, and we can try out every one of the twenty-six possible positions of the two series of letters. Thus, suppose we start right in with $A_p = Z_c$:

English - A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Cipher - Z Y X W V U T S R Q P O N M L K J I H G F E D C B A

Try out the first two groups of the cipher message.

Cipher - LXAER ETGLW
"English" - OCZVI VGTOD $A_p = Z_c$

This certainly isn't English, so we move the lower strip one space to the right. Thus:

English - A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Cipher - A Z Y X W V U T S R Q P O N M L K J I H G F E D C B

Try for solution again:

Cipher - LXAER ETGLW
"English" - PDAWJ WHUPE $A_p = A_c$

More Trials

Neither is this English. Once more:

English - A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Cipher - B A Z Y X W V U T S R Q P O N M L K J I H G F E D C

Try for solution once more:

Cipher - LXAER ETGLW
"English" - QEBXK XIVQF $A_p = B_c$

Nothing doing--but just look at the results of the three tests. Let's put them under one another:

	Cipher -	LXAER	ETGLW
Result of 1st test	$A_p = Z_c$ -	OCZVI	VGTOD
" " 2nd "	$A_p = A_c$ -	PDAWJ	WHUPE
" " 3rd "	$A_p = B_c$ -	QEBXK	XIVQF

Figure 15.

The letters in the columns after the first test go in direct alphabetical order. Suppose we continue the sequences a couple more times. Thus:

Cipher -	LXAER	ETGLW
$A_p = Z_c$ -	OCZVI	VGTOD
$A_p = A_c$ -	PDAWJ	WHUPE
$A_p = B_c$ -	QEBXK	XIVQF
$A_p = C_c$ -	RFCYL	YJWRG
$A_p = D_c$ -	SGDZM	ZKXSH
$A_p = E_c$ -	THEAN	ALYTI

Figure 16.

Eureka! We have it! The method does work after all. In what way is this diagram different from those in Figures 9 and 10? In only one way. Instead of setting the alphabet strips up according to the cipher letters right away, if you first set a reversed alphabet against the ordinary alphabet, "translate" the first two groups of your cipher message, and then set up these new letters on the ordinary alphabet strips, you'll get the solution. You only have to do this with the first two or three groups in order to get the start on the solution, because once you've made a start you can use your revolving disks to solve the rest of it. To show you what I mean, I will go through the steps for this particular example.

Coat Of Many Colors

Having found that the first cipher group LXAER equalled English THE AN..., this means that $L_c = T_p$. Now merely set your revolving disks (remember we're now using one reversed sequence against the ordinary sequence) so that $L_p = T_c$, and see what A_p equals. You will find that $A_p = E_c$. That is the key letter, and by that setting of

the disks you can decipher the whole message without any difficulty and without having to use the sliding strips.

Get these steps straight in your mind and then tackle the next problem.

Problem 4

YKNVA JYYNE GRELX RLNZD MYKNF RIDAJ YTDMP JWJGJ

SNOCN DCGNZ DMYDO RTRAN RGCKR QNYJP RGJEE RYXAN

Problem 4 was solved (if you really have solved it, and I think you have) by means of one and the same setting of the revolving disks, for the whole message. Now suppose that the disks are moved to different settings in enciphering one message--just as was the case in Example 2 and Problem 3. What would you do to solve such a message?

Begin To Get The Drift

Well, first let us see how such a message is enciphered. Suppose A and B decide to change the setting of their revolving disks after every five letters, using the word SECRET as a key. Let the message be "COME IMMEDIATELY. HAVE IMPORTANT NEWS". Check up on the following encipherment and make sure you understand it.

Example 5.

Key	-	$A_p=S_c$	$A_p=E_c$	$A_p=C_c$	$A_p=R_c$	$A_p=E_c$	$A_p=T_c$	$A_p=S_c$
English	-	COMEI	MMEDI	ATELY	HAVEI	MPORT	ANTNE	WS
Cipher	-	QEGOK	SSABW	CJYRE	KRWNJ	SPQNL	TGAGP	WA

Now let's go through the solution of this example just as if we didn't know that the keyword was SECRET.

First. Set your revolving disks A to A and "decipher" all the letters of the message. Of course the result won't be English (except by accident) but it is one step in the process. Here is the result:

Message	-	QEGOK	SSABW	CJYRE	KRWNJ	SPQNL	TGAGP	WA
Deciphered $A_p = A_c$	-	KWUMQ	IIAZE	YRCJW	QJENR	ILKNP	HUAUL	EA

Now set up as many of your sliding strips as you have, bringing these newly obtained letters all on the same horizontal line. Then begin to look for English. Thus:

Figure 17.

K	W	U	M	Q	I	I	A	Z	E	Y	R	C	J	W
L	X	V	N	R	J	J	B	A	F	Z	S	D	K	X
M	Y	W	O	S	K	K	C	B	G	A	T	E	L	Y
N	Z	X	P	T	L	L	D	C	H	B	U	F	M	Z
O	A	Y	Q	U	M	M	E	D	I	C	V	G	N	A
P	B	Z	R	V	N	N	F	E	J	D	W	H	O	B
Q	C	A	S	W	O	O	G	F	K	E	X	I	P	C
R	D	B	T	X	P	P	H	G	L	F	Y	J	Q	D
S	E	C	U	Y	Q	Q	I	H	M	G	Z	K	R	E
T	F	D	V	Z	R	R	J	I	N	H	A	L	S	F
U	G	E	W	A	S	S	K	J	O	I	B	M	T	G
V	H	F	X	B	T	T	L	K	P	J	C	N	U	H
W	I	G	Y	C	U	U	M	L	Q	K	D	O	V	I
X	J	H	Z	D	V	V	N	M	R	L	E	P	W	J
Y	K	I	A	E	W	W	O	N	S	M	F	Q	X	K
Z	L	J	B	F	X	X	P	O	T	N	G	R	Y	L
A	M	K	C	G	Y	Y	Q	P	U	O	H	S	Z	M
B	N	L	D	H	Z	Z	R	Q	V	P	I	T	A	N
C	O	M	E	I	A	A	S	R	W	Q	J	U	B	O
D	P	N	F	J	B	B	T	S	X	R	K	V	C	P
E	Q	O	G	K	C	C	U	T	Y	S	L	W	D	Q
F	R	P	H	L	D	D	V	U	Z	T	M	X	E	R
G	S	Q	I	M	E	E	W	V	A	U	N	Y	F	S
H	T	R	J	N	F	F	X	W	B	V	O	Z	G	T
I	U	S	K	O	G	G	Y	X	C	W	P	A	H	U
J	V	T	L	P	H	H	Z	Y	D	X	Q	B	I	V

The English words come out on different lines, as you notice in Figure 17, five letters at a time. Simple enough, isn't it? Of course the correspondents can agree on almost any kind of a method of changing the setting of their disks in enciphering. They could agree to change the setting after every sentence, or after every word, after every group of ten, five, three, two, or even one letter--but then it gets much harder as the lengths become reduced. We'll see about that later. At any rate, in the next problem you won't find anything so difficult.

Oh, I almost forgot to show you how to find the keyword--if you're curious. You just take your revolving disks and reset them each time the English comes out on a different line in the "set-up" of the sliding strips. See what A equals, and that gives you a letter of the key. For instance, in the foregoing example, we found that cipher letters QEGOK equalled COMEI, and then the key changed. Here Q equals C, and the same setting was used for the five letters. So set your two revolving disks so that Q equals C and you will see that A equals

Seeing What Makes The Wheels Go Round

S. That's the first letter of the key. Then you take the next group of letters enciphered by a different setting. They are SSABW, and equalled MMEDI. Here S equals M. Set the disks accordingly and you find that A equals E. That's the second letter of the key, so we now have SE as the beginning of the key. Well, I think you won't need any further explanation of how to get the rest of it. If you think you do, better dig it out for yourself.

All right now. Are you ready for the next problem?

Problem 5

TFKWZ ALRIZ HEBMQ ZETER LXRLN RANFN VIDQV HHDRT HJDWR ELWQR ZREOC

NAFXY MTGAB WHQRK RJARL ENGMQ XEOZV KJPKK MRKNQ DHIPB DVYAD ACQSA

ANPDL EJSNO MZLOL AGCRS VDLXA NAPNA ZNEYR YJWNZ YHLKJ GINCR HUVAC

LMQNW ONRZU

Did you find the key?

Well, you've been having a pretty easy time of it so far. Once you got on to the tricks with the sliding alphabets there was nothing to it. There wasn't anything to cause you to chew the end of your pencil, and to use your eraser very much.* The reason is that the

---

* There's an electric eraser, to be had, if you're getting all hot and bothered. Zoom! And a whole line is wiped out. Honest!

Ah! This is Something Else Again

cipher alphabets that we've used so far were merely ordinary alphabets, that is, the natural order of the letters was not changed at all in these alphabets. But now you're in for it. We're going to mix up the alphabet, and, believe me, that's going to gum the game with those sliding strips. However, don't throw them away just yet.

First, to show you how a message is enciphered. Suppose A and B decide to communicate in cipher by means of the following alphabet:

English - A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Cipher - P R E S I D N T Z A C H Y L O B F G J K M Q U V W X

Take a good look at that lower line, by the way. It looks as if there's a name in it, doesn't it? Yes, there is--PRESIDENT ZACHARY TAYLOR. This represents a simple way of getting a mixed alphabet without having to keep written notes on you. All you have to do is to keep in your head the secret keyword, or key name, or key phrase, and then whenever a cipher message is to be prepared or translated, you can write out the alphabet without any trouble and without having to carry around any dangerous slips of paper. First you write the key, using each different letter only once. Then you follow it up with the rest of the unused letters of the alphabet. So, you see, when the second E in PRESIDENT comes, you just omit it and go right on with NT. Then comes ZACHARY. The second A in ZACHARY is omitted, and also the R, because they have already been written down. TAYLOR gets reduced to a mere LO; then you start in with B, then comes C, but C is already in, and so are D and E. F is the next letter, and so on until you've completed the alphabet. The longer the key is, and the more different letters it contains, why the more disarranged the alphabet becomes. This type is called a keyword alphabet.

Another Useful Term

So much for the alphabet. The method of enciphering the message is just the same as before. For example, COME IMMEDIATELY. HAVE IMPORTANT NEWS would be put into cipher, by means of the cipher alphabet just given, as follows:

COMEI	MMEDI	ATELY	HAVEI	MPORT	ANTNE	WS
EOYIZ	YYISZ	PKIHW	TPQIZ	YBOGK	PLKLI	UJ

We are getting out of the primer class now. That system we used as members of the Way-Back-When Crime Club doesn't appear so wonderful now.

CHAPTER IV

The Class Will Please Come To Order

I don't have to show you how to decipher such a message--when you have the alphabet or the key upon which it is based. What you want to learn is how to do it without the alphabet or key. I think a good practical way is to take you with me through the steps in solving an example. Suppose we have this one to do:

Example 5.

MTWEG IIGDR LSPYG MQMRG LEHGO MTWSG IZVYS RLMTW AHWCW LMXQC WRLZW

WZRLQ IIXQC WCGEC WXHWM DHRMR LSMTW ERHCM PYWCM RGLHW SQHZC MTWIQ

LSYQS WGEMT WXRAT WHEGH MTWAH RLXRA IWCGE CGIYM RGLCG EQHWC AWXRQ

JIJQC MTWOG HWCRO AIWXR ATWHC QHWXG LXWHL WZZWA WLZGL QLZQH WBQHR

WZVJM TWSWL RYCGE MTWAQ HMRXY IQHRZ RGO

Now you can solve this problem in two ways. I used to work for a man, who, though he wasn't a scientist himself, had many in his employ ('twas ever thus!) and had the scientific spirit. One of the things that would irritate him, and you could always be sure to get a rise out of him by so doing, was to tackle any kind of a job (in his words), "By guess and by God." Well, that's one way you can tackle this problem and probably solve it in time. You could simply make a single count of all the letters, and replace the most frequent one by E, the next most frequent one by T, and so on, according to pure frequency. Then by cut and try methods,

Dumb Blind Persistence

much use of the rubber end of your pencil, and considerable fuming, you'd ultimately get it. (If you're that kind of a workman, and a poor guesser to boot, remember what I said about the electric eraser).

But I really think you'd rather go at it in the scientific way. It may seem to be a little slower at the start (so is all good work), but you'll save time in the end. So, have patience, and watch your step.

First, we make a new kind of a frequency table for the message. The kind that you've seen so far merely showsyou what letters are present, and how many of each. The kind we're going to make will not only show these two things, but will also show what combinations of two and three letters occur, and how many of each.combination. This information is very useful. You know the old saying about judging character by the company a fellow keeps. Well, it's the same principle here. By watching the gang a certain letter plays around with, you can tell better who the fellow is. The table we are going to compile is for the purpose of finding out what company each letter keeps. The table, by the way, is technically known as a trigraphic frequency table, from the word trigraph, meaning a set of three letters.

Inside Dope

Here's how it's made. Take some ruled paper and write the alphabet at the bottom of it, horizontally. Now every letter in the message has a letter before it, and a letter after it, except the first (which doesn't have one before it) and the last (which doesn't have one after it). Above each letter on the sheet there will finally appear two columns of letters: the left hand column will show the letters that precede every letter in the message; the right hand column, those that follow. Take the first letter in the message, M. It has no letter

before it, but it is followed by T. Therefore, above M, we write -T, which indicates that the first time M occurs it begins the message, and it is followed by T. Thus:

```
                        -T
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
```

The next letter in the message is T; the letter before it, M, the letter after it, W. Therefore, above T we write MW. Thus:

```
                        -T            MW
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
```

The next letter is W; letter before it, T, after it, E. Therefore:

```
                        -T            MW    TE
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
```

And so on. When you get to G, the last letter of the first group, you have EI above it, because I follows G in the message--you don't stop between groups. This is what you get for the whole message:

Figure 18.

Very Impressive

Letter	Count	Entries (top to bottom)
A	9	WQ WW RT OI CW RI WH RT WH
B	1	WQ
C	16	YG HQ WR QM WA LG EG WG ZM WM HM EW WG QW QW WW
D	2	MH GR
E	9	GM GQ GC HG GM WR GC LH WG
F		
G	19	RO CE ZL XL OH CE RL CI CE EH WE RL CE SI HO RL YM ID EI
H	19	QR QM QR QW WL QW WC GW QW AR GM WE QZ LW RC DR XW AW EG
I	12	YQ AW IJ QI GY AW WQ IX QI GZ IG GI
J	2	VM IQ
K		
L	17	WR QZ GQ WZ HW GX GC RX QS GH RS RQ RZ WM RM GE RS
M	19	HR ET JT CT YR HT ET CT CR CP ST RR WD LX LT OT QR GQ -T
N		
O	4	G- RA WG GM
P	2	MY SY
Q	16	IH AH BH ZH LL CH JC RI EH YS IL SH XC LI XC MM
R	21	ZG HZ MX LY HW XA CO XQ MG XA HL XA MG EH ML HM ZL WL SL MG DL
S	8	WW QW LY WQ LM YR WG LP
T	12	MW MW AW MW MW AW MW MW MW MW MW MW
U		
V	2	ZJ ZY
W	36	TA SL TS RZ HB AL ZA LZ XH HX TH IX HC TO AX HC IC TA TH TX SG TI HS YC TE HM CX CC WZ ZW CR CL HC TA TS TE
X	10	RY LW WG WR WR LR WR WH IQ MQ
Y	7	XI RC IM SQ PW VS PG
Z	10	RR WV LQ LG ZW WZ HC WR LW IV

Merely Scenery?

Now that we've got the thing, what on earth do we do with it? Well, just this: we can use it as a scientific basis for assuming values for not only single letters but also for pairs of letters, and groups of three or more letters. Furthermore, even in assuming values for single letters your work can be much more accurate than without this tool.

It is like this. Not only is it true that individual letters of the alphabet have characteristic frequencies, but it is also true that letters combine in a more or less characteristic way to form pairs, triplets, and so on. A pair of letters is usually called a digraph, a set of three letters, (as I said once before) a trigraph. Now the table we have just made, Figure 18, will show exactly what digraphs and trigraphs occur in the message. For example, take the frequency of A_c, which is shown here at the right. The digraph WA_c occurs four times, RA_c occurs three times, CA_c and OA_c once each. The digraphs AH_c, AI_c, AT_c, and AW_c occur two times, and AQ_c only once. The trigraph WAH_c occurs twice; that is, wherever the same pair of letters occurs in the two columns standing above a letter, that means a repetition of a set of three letters. Now you can find all the repeated digraphs by examining either the right hand columns above each letter, or the left hand--you will get the same results, providing only you do it consistently. That is, if you start off to list the repeated digraphs by examining the right hand column of the first cipher letter in the table, you should stick to the right hand column all the way through. To show you that you'd get the same results, take the pair WA_c, which we found, by examining the left hand column above A_c in

What Now?

WQ
WW
RT
OI
CW
RI
WH
RT
WH
A

Figure 18, occurs four times. If you'll look through the letters in the right hand column above W_c, you will find A_c occurs exactly four times, meaning WA_c occurs four times. It is not necessary to list every digraph that occurs or is repeated. Only the most frequent digraphs and trigraphs need be listed, and I have listed below the most significant ones of Figure 18:

DIGRAPHS			TRIGRAPHS
TW - 12	CG - 5		MTW - 10
MT - 10	GE - 5		CEG - 4
HW - 7	GL - 5		QHW - 3
QH - 7	MR - 5		TWA - 3
RL - 6	WX - 5		HWC - 3
WC - 6			WXR - 3

Now let us apply this information to the problem in hand. You will recall that I mentioned the fact that letters combine to form pairs which have characteristic frequencies, and in Figure 19, the relative frequencies of many common pairs are given. The information offered by this table will be of considerable use to you. You will

Harder Sledding

Figure 19.

Most Frequent Digraphs			Most Frequent Trigraphs	
TH - 50	AT - 25	ST - 20	THE - 89	HAS - 28
ER - 40	EN - 25	IO - 18	AND - 54	NCE - 27
ON - 39	ES - 25	LE - 18	THA - 47	EDT - 27
AN - 38	OF - 25	IS - 17	ENT - 39	TIS - 25
RE - 36	OR - 25	OU - 17	ION - 36	OFT - 23
HE - 33	NT - 24	AR - 16	TIO - 33	STH - 21
IN - 31	EA - 22	AS - 16	FOR - 33	MEN - 20
ED - 30	TI - 22	DE - 16	NDE - 31	
ND - 30	TO - 22	RT - 16		
HA - 26	IT - 20	VE - 16		

notice the most frequent trigraph in English literary text as shown in Figure 19 is THE, and the most frequent digraph is TH. The TH is usually very easy to find because of one funny thing about it. Although as a pair it is by far the most frequent of all pairs, and although the first letter, T, is one of very great frequency, the

Oh Man! The Real Stuff

second letter of the pair, H, is one of the medium or low frequency, and moreover, it is nearly always preceded by T, and is many times followed by E. Thus, in examining a trigraphic frequency table you can nearly always spot the cipher equivalent of THE by looking over the repeated trigraphs for one that (1) has as its middle letter one of low or medium frequency, (2) is nearly always preceded by the same letter, and (3) is often followed by the letter of highest frequency. Take a look at the list of repeated trigraphs given for our problem. The trigraph MTW occurs ten times; T_c is of <u>medium</u> frequency; it is nearly always preceded by the same letter, M_c of <u>high</u> frequency, and is nearly always followed by W_c, the letter of <u>greatest</u> frequency. T_c occurs twelve times in all; ten times it is preceded by M_c, and every time it is followed by W_c. It is easy to see that MTW_c is almost certain to be THE_p.

As to the other trigraphs listed for our problem, repetitions of three and four times do not give much information as yet. Nor do the repetitions of the digraphs. TW_c, we saw equals HE_p, and MT_c equals TH_p.

Surely you know what are vowels and what are consonants?

Now I think you will realize that it would be very much of a help if we could find out which cipher letters stand for vowels, and which stand for consonants. I am going to show you how you can find out this interesting bit of information from the frequency table alone.

Make a list of the ten letters of highest frequency:

36W 21R 19G 19H 19M 17L 16Q 16C 12I 12T

We have already decided that W_c equals E_p, T_c equals H_p, and M_c T_p, so that we can eliminate them from the list. Now find out how many times each of the remaining high frequency letters combines with

W_c, which we know is a vowel. For example, the table shows that WR_c and RW_c occur only once; WG_c only once; GW_c not at all; WH_c, three times; HW_c, seven times; and so on. Just put marks above each letter in the foregoing list to show the number of combinations with W_c. Like this:

Figure 20.

W_c precedes: -							
Letters : -	21R	19G	19H	17L	16Q	16C	12I
W_c follows : -							

(carbon has figures and letters above in Fig. 20)

Now if you will examine carefully Figure 19, on page 00, you will see that combinations of E_p with the high frequency consonants N, R, S, and T are much more frequent than combinations of E_p with other vowels. Hence, in Figure 20 where there is indicated the number of times certain cipher letters combine with W_c (which equals E_p) it would follow that R_c, the letter of second highest frequency, stands for a vowel because it combines with W_c (which equals E_p) so seldom; likewise G_c seems to stand for a vowel. On the other hand, H_c seems to represent a consonant, because it combines so frequently with W_c (= E_p). Likewise, L_c seems to represent a consonant, for the same reason. Q_c, however, would seem to stand for a vowel. C_c is certainly a consonant. We can neglect I_c for the present. Thus, we have:

Slow! Dangerous Curve

W_c		H_c	
R_c		M_c	
G_c	represent vowels	L_c	represent consonants
Q_c		C_c	
		T_c	

Now then, look sharp. Among the cipher letters that we have just classed as standing for vowels, W_c is E_p; hence R_c, G_c, and Q_c must represent A_p, I_p, and O_p, but which is which? Well, among the

pairs of vowels that can be made from the four vowels A, E, I, and O, in English only the pairs EA, IO, and IE are frequent at all. (Check this by referring to Figure 19, page 00). Three of these contain E as one of the letters. So let us see what pairs occur with the letters W_c, R_c, G_c, and Q_c in our problem.

WR - 1	RW - 1	GW - 0	QW - 0
WG - 1	RG - 4	GR - 0	QR - 0
WQ - 0	RQ - 1	GQ - 0	QG - 0
WW - 1	RR - 0	GG - 0	QQ - 0

The combination RG_c, four times, cannot be either EA_p, or IE_p, because if either of these were true then R_c would have to equal E_p and we have already decided that W_c is E_p. The only other high frequency vowel combination not containing E is IO, and hence RG_c must be IO_p. That means, R_c equals I_p, and G_c equals O_p. By elimination, then Q_c must be A_p. Thus we have:

$W_c = E_p$ $R_c = I_p$ $G_c = O_p$ $Q_c = A_p$

Now IO_p in English is most often followed by N_p in the frequent ending ION; and the ending TION is one of the most frequent of all four-letter endings. If RG_c is really IO_p, and since we long ago decided that M_c equals T_p, we should find a set of four cipher letters, MRG-, occuring several times in the message. Look at the text and you will see that $MRGL_c$ occurs three times. Hence, L_c must be N_p. You will also remember that we classified L_c as a consonant. So now we have

$W_c = E_p$ $R_c = I_p$ $G_c = O_p$ $Q_c = A_p$ $M_c = T_p$ $T_c = H_p$ $L_c = N_p$

The cipher equivalents of only two more high frequency letters must be found now - those for R_p and S_p. We classified H_c and C_c as consonants. From frequency considerations H_c looks R_p, and C_c

looks like S_p, but we can't as yet be sure - it may be the other way around. So let us include them in our list as alternative values.

$W_c = E_p$ $R_c = I_p$ $G_c = O_p$ $Q_c = A_p$ $M_c = T_p$

$T_c = H_p$ $L_c = N_p$ $H_c = R_p$ or S_p $C_c = S_p$ or R_p

Well, now, it looks as if we've built up a lot of guesses - nothing has yet been tested on the message. It's high time we did so, don't you think? Suppose our values gave us some perfectly impossible

Hold combinations? I mean, for example, such things as --AAEO-- and

Your --RTNTS-- and so on, which are impossible in English. But if we

Breath are on the right track our trials should not give such impossibilities.

Let's see.

MTWEG THE O	IIGDR O I	LSPYG N O	MQMAG TATIO	LEHGO N RO S	MTWSG THE O	ISVYS	RLMTW INTHE	AHWCW RESE S R
LMXQC NT AS R	WRLZW EIN E	WZRLQ E INA	IIXQC AS R	WCGEC ESO S R R	WXHMW E RET S	DHRMR RITI S	LSMTW N THE	ERHCM IRST SR
PYWCM EST R	RGLHW IONRE S	SQHZC AR S S R	MTWIQ THE A	LSYQS N A	WGEMT EO TH	WXRAT E I H	WHEGH ER OR S S	MTWAH THE R S
RLXRA IN I	IWCGE ESO R	CGIYM SO T R	RGLCG IONSO R	EQHWC ARES S R	AWXRQ E IA	IIJQC AS R	MTWOG THE O	HWCRO RESI S R
AIWXR E I	ATWHC HERS SR	QHWXG ARE O S	LXWHL N ERN S	WZZWA E E	WLZGL EN ON	QLZQH AN AR S	WBQHR E ARI S	WZVJM E T
TWSWL HE EN	RYCGE I SO R	MTWAQ THE A	HMRXY RTI S	IQHRZ ARI S	RGO IO			

The Look at that! No impossible combinations are found. The skeletons

Thrill of words shine out and make you jump, I'll wager. Only it's joy,

Of not jitters. So let's finish it. You can fill in many words

Your from mere inspection. For example, the second word in the message,

Life EGIIGDRLS -O--O-IN-, with a double letter (II) in it looks like the word

FOLLOWING, and gives four new values: $E_c = F_p$, $I_c = L_p$, $D_c = W_p$, and $S_c = G_p$. H_c seems to be R_p quite clearly, and $C_c = S_p$. And so on. It's all very simple from now on. Once you get five or six of the high frequency letters correct, the whole thing falls like a house of cards. But you've got to get the first few right, otherwise you'll lose a lot of time. It pays to go very slowly at the start, using your best judgement for every letter. Above all, don't jump at conclusions too quickly, or you'll surely stub your toes. Neither must you stick too closely to the frequency table. Remember that E is not <u>always</u> the most frequent letter in a message, nor is T <u>always</u> the second highest in frequency. Be ready to throw overboard any assumption that doesn't give you good results after careful work, and make another assumption in place of it. (No, I'm not contradictory and saying, "Do it, Don't do it" : - with a little experience you'll get what I'm driving at.)

Well, here is the complete solution to the message; notice that there is no punctuation - you have to supply that, as a rule, in practical work: THE FOLLOWING QUOTATION FROM THE GOLD BUG IN THE PRESENT CASE INDEED IN ALL CASES OF SECRET WRITING THE FIRST QUESTION REGARDS THE LANGUAGE OF THE CIPHER FOR THE PRINCIPLES OF SOLUTION SO FAR ESPECIALLY AS THE MORE SIMPLE CIPHERS ARE CONCERNED DEPEND ON AND ARE VARIED BY THE GENIUS OF THE PARTICULAR IDIOM

And here is the cipher alphabet:

English - A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Cipher - Q V X Z W E S T R N U I O L G A P H C M Y B D F J K

The Eternal Keyword

Can you see any key word or phrase in the cipher alphabet. How about WESTERN UNION TELEGRAPH COMPANY? But why doesn't the alphabet start right out with the WESTERN etc? Why with Q? Well, for the

simple reason that if you have the cipher series on a strip of paper that you can slide back and forth, you can use the same key sequence to make a whole set of twenty-six cipher alphabets. That is, you could write the same message in twenty-six forms of cipher, all different, merely by sliding the same mixed alphabet to different positions against the normal. Historically, this is known as the Vigenere Table, from a French cryptographer of that name, or the Chiffre Carrè, or the Square Cipher. It was considered the tops in Vigenere's day.

But once you've found one of these cipher alphabets you can decipher any message written by any of the other cipher alphabets belonging to the same set and you can do it in a hurry. It's quite a useful trick and I'll let you in on it. I won't explain it in detail. I'll just show you an example and let you figure it out, because it's more fun if you do it yourself.

Let's suppose that the message we just deciphered is one of a series passing between two correspondents. Here's another one, very short:

OQVIV IMIVE RWFIL YIOVO LOVTS BVRQF U

First step - Writing down the cipher alphabet:

English - A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Cipher - W E S T R N U I O L G A P H C M Y B D F J K Q V X Z

Short Cut

Second step - Reducing the cipher letters to ordinary alphabet equivalents by means of the known cipher alphabet:

Cipher - OQVIV IMIVE
"English" - IWXHX HPHXB

Third step - Completing the columns by the ordinary alphabet and looking for plain text:

Cipher -	O	Q	V	I	V		I	M	I	V	E
	I	W	X	H	X		H	P	H	X	B
	J	X	Y	I	Y		I	Q	I	Y	C
	K	Y	Z	J	Z		J	R	J	Z	D
	L	Z	A	K	A		K	S	K	A	E
	M	A	B	L	B		L	T	L	B	F
	N	B	C	M	C		M	U	M	C	G
	O	C	D	N	D		N	V	N	D	H
	P	D	E	O	E		O	W	O	E	I
	Q	E	F	P	F		P	X	P	F	J
	R	F	G	Q	G		Q	Y	Q	G	K
	S	G	H	R	H		R	Z	R	H	L
Figure 19	T	H	I	S	I		S	A	S	I	M
	U	I	J	T	J		T	B	T	J	N
	V	J	K	U	K		U	C	U	K	O
	W	K	L	V	L		V	D	V	L	P
	X	L	M	W	M		W	E	W	M	Q
	Y	M	N	X	N		X	F	X	N	R
	Z	N	O	Y	O		Y	G	Y	O	S
	A	O	P	Z	P		Z	H	Z	P	T
	B	P	Q	A	Q		A	I	A	Q	U
	C	Q	R	B	R		B	J	B	R	V
	D	R	S	C	S		C	K	C	S	W
	E	S	T	D	T		D	L	D	T	X
	F	T	U	E	U		E	M	E	U	Y
	G	U	V	F	V		F	N	F	V	Z
	H	V	W	G	W		G	O	G	W	A

Fourth step - Setting the alphabet for the message in hand, according to the solution of the first group:

$$O_c = T_p$$

English -	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher -	M	Y	B	D	F	J	K	Q	V	X	Z	W	E	S	T	R	N	U	I	O	L	G	A	P	H	C

Fifth step - Deciphering the rest of the message:

OQVIV	IMIVE	RWFIL	YIOVO	LOVTS	BVRQF	U
THISI	SASIM	PLESU	BSTIT	UTION	CIPHE	R

What chance would you have had of solving this short cipher by any other method? Hardly any - as yet; an expert could do it, but even he ~~would~~ might have a hard time with it. But if you have the original key alphabet, or the words upon which it is based, then it is easy. So goes Progress. What was beyond the horizon yesterday, may be within our grasp today.

CHAPTER V

Itching To Try Your Hand?

Well, are you ready to try your hand at solving one now? If you think so, go to it. And I might as well tell you that it isn't anything taken from Edgar Allen Poe's Essays.

PROBLEM 6

LXRRS IRNOZ RMRWO YUEUX LELQO ZBZOZ UGRWO YUXRB UNMAU MOZMS

UUSLE ERWOY RGUPU LNZMX VIRMO YUQRN NUQOS ZGQYL NXURW OYULS

AZMZG ONLOZ RMSVO ZUGRW OYUUF UQVOZ BUSUI LNOAU MOGLG DUEEL

GRWOY UZMSU IUMSU MOUGO LPEZG YAUMO GZGQR MSVQO USDZO YRVOQ

LEEZM XVIRM OYULO ORNMU JXUMU NLEWR NLGGZ GOLMQ U

To each and every man, woman, or child who can find the word or phrase upon which the cipher alphabet for Problem 6 is based I offer as a reward one pair of genuine cork-tipped spectacles for his or her pet household mouse. That's how hard it is.

After adjusting the said spectacles, try the next one, and you'd better examine very carefully the steps illustrated on page 00.

PROBLEM 7

PAWJM FJATI TEVAD WFTOH VDOXC TNFMQ

To give you a little more practice in the work of solving this type of cryptogram I am going to add several more problems just like it. I warn you beforehand, however, that they get harder and harder

Blessings On Thee

because they become shorter and shorter. You'll learn by actual experience that the shorter a message is, the longer does it keep you working. Furthermore, I might as well tell you that there will be very few "THEs" in these messages. People who spend good money to telegraph messages leave out all unnecessary words, and "THE" can most easily be left out. You will have to use more ingenuity in making the first break into solution because of the absence of "THE". You can make good use of the method I showed you for separating the vowels from the consonants, though, and that ought to help considerably. Another pointer: Build up the cipher alphabet as you go - it will help you in more ways than one. A word to the wise is sufficient.

A word to the wise

PROBLEM 8

YVAVN MRSNU VNACW PVNSA VMWVN GQMAV JHVUG BGSAM NKXSN QVTFM TGTTC

VUGAY VAVNM RHVNT ZGAYT BFSNS SWSXX GQVBF SKVMN TRMBV NFGBZ DGQBS

NKMQQ SWHRG TZVUM AUBZV WGRRG SATSX KSCAY MWVNG QMATN VTBSN VUBSQ

GDGRR GXVVJ QVHBX SNBZS TVFZS TRVHB GATSR UGVNY NMDVT GAXNM AQVSN

MBZSW VBZVR MTBYV AVNMR SNUVN MRTSF MTGTT CVUPK YVAVN MRHVN TZGAY

GAFMT ZGAYB SAGBU GTPMA UVUBZ VMWVN GQMAV JHVUG BGSAM NKXSN QVT

Now don't look up the answer to Problem 8 until <u>after</u> you've solved Problem 9!

Beware

The next one, Problem 9, uses the same key as a basis for mixing the alphabet, only the cipher sequence is slid to a different point. Follow the steps illustrated on Page 00 and in Problem 7.

PROBLEM 9

WBPGA GUBLI AHEKW XKCFB YIEND

PROBLEM 10

HYPJV OCVOJ HUGZU VNYCN CHWJH YWJHC LLJZH VJXJN UVOHC LRJXM SYYFY

TSYCN UJFZV YFRTY XZUYU VJLJH UOWYT CHRVS OHPFY UUVSC HUSCT YCHWU

SCTYC FODYJ HCFFT YLYOK VUZHF YUURJ ZLCHC ZVSJT OIYUC GYMOF FWTJK

CFFHY PJVOC VOJHU NRXTO WCRHJ JHCHW TYVZT HSJGY

Problem 11 is another one like Problem 7 and Problem 9, only the alphabet is based upon the one you've just built up by solving Problem 10.

PROBLEM 11

JCIUJ BMNZS LTJGP MFVMV SUUNF

PROBLEM 12

PCVSL QKNJS RSEVS IEATD JBCNE DAWPE RPBCU SKENC IVEKC HMSTD JYDQN

DJSNQ JACNS CJMES KNFDK KEHMS ICNSW EJSBS EBBSI ECNSM YWPSA YDQRC

AOSNC WCYCA IWEMM NSMSO JCFPT QAIKT DJNJC VSMXX

Using the alphabet built up as a result of solving Problem 12, solve the next one.

PROBLEM 13

WQPTY QFYOQ MWHBY FYPAH

PROBLEM 14

LCURH FJMHK PLRCQ QCLAC ZCJQY AQSQP AESAC JKQBC IFJFQ CRHBC QCLGF

JCBRP QRKKO AGKAQ ISZKL SDRCQ KERFC JQXFR ROCCU HKPFJ IKLGG BSJHJ

CXBCZ CRKUG CJQAW

Using the alphabet built up as a result of solving Problem 14, solve the next one - and try to answer the question it asks.

PROBLEM 15

IGPPH TLIEH NJIHV ELBGU JUGVN EOBGA ULEER CHDEK

Now then. They're getting pretty short, aren't they? Here's a challenge to your ability. The next three problems (16, 17, and 18)

are all in exactly the same alphabet, no sliding or anything else.

Heavy Artillery

They are all of the same length. Try your hand at solving just the first one, without any reference whatsoever to the other two. You can do it if you try hard enough. Now if after you've struggled with it, and have run out of the proper sort of epithets, and are ready to give it up, then try the second one alone. Maybe you can knock that one for a goal. Then, if you're still unsuccessful, try the third one alone. If you still don't get anything, combine the frequency tables for any two of them and try once more. Finally, if that doesn't work, combine all three into one problem - you're sure to get them in that way. But just see how good you are first and do as I suggest - and "no fair peekin" at the ones you're not supposed to look at. (This is a new-fangled honor system.)

PROBLEM 16

MJTQS QWQSS QPYUC LDCSQ GQTYQ SPJGM UEQTA IYUEU SSUDJ NNTQY

PROBLEM 17

MJTQJ XJCLI UTYIU LQPUL JMMUA LYCNN LQTTC EIUSY JLYDC YLQTT

PROBLEM 18

MJTQP QMCPQ PJXJC LTYGU AEAMZ PCTJI IUCLY QPJPB CTQJI IQJNF

There are many changes that can be rung on this simple substitution type, without making the solution much harder. In the next few examples, I will illustrate some of them.

Of course, now that you understand how to solve this type of cryptogram, ciphers like those in Poe's "Gold Bug", and in Conan Doyle's " Sign of Four" should give you no trouble at all. As I said in the opening pages, cryptograms that use anything but letters, or occasionally figures (but never mixed in the same message) are hardly ever used in serious cryptographic correspondence. If you

come across any like that, for example, with all kinds of funny signs, punctuation marks, dancing men pictures, and so on, it's a sure sign the thing was put up by a simple-minded amateur. The easiest thing to do in such a case is to substitute letters for the different characters and then treat the thing just as if it were originally a letter cipher, pure and simple. Of course, if the thing comes with the original word lengths indicated, it can be read almost at sight, because it's so easy to pick out and solve the short words such as "to", "by", "of", "and", "in", and so on. Honestly, I'm sure that after you've solved the ones in this book you won't have much patience with that sort. What I want to give you here is a little information on some of the more common variations that are often used by people who think they're making the thing very complex.

Here's a variation that you should know. Suppose I make a diagram like this, where the letters of the alphabet are inside the small squares, and the cipher equivalent of a letter is given by the two letters which mark the square the letter that is being enciphered occupies. For example, letter R_p would here be represented by CL, and the word REPORT would be enciphered as

	B	L	A	C	K
B	A	B	C	D	E
L	F	G	H	I J	K
A	L	M	N	O	P
C	Q	R	S	T	U
K	V	W	X	Y	Z

Figure 22

R	E	P	O	R	T
CL	BK	AK	AC	CL	CC

You will notice that I and J occupy the same square and have the same value.

A cryptogram like that might mystify you at first because it would contain only five different letters, but you should soon

New Tunes On Old Themes

realize that with only this number of different letters the most usual thing is that each English letter is represented by a pair of cipher letters. Then, to solve such a cipher you must first divide it up into pairs of letters, and you will usually find that there are only about 20 to 25 different pairs, depending on how many letters of the alphabet were used in the clear-text message. You can then assign a single letter to each different pair and go ahead as before, just the same as though it were a simple, single-letter cipher.

In the diagram I've shown (Figure 22) the letters in the squares are in regular order, so that if you find the value of only one cipher pair you have excellent clues to the values of nine other letters. For example, using the diagram above, suppose you've found that the combination BK stands for E_p. Then you can see that the cipher combination for A, B, C, and D must all start with B, and the cipher combination for K, P, U, and Z must all end with K. So the fact that the letters are in regular oder in the squares is of great help in solution. Try this one and see for yourself:

PROBLEM 19

Got UIQQT QQTQE QCEIQ IIETQ QTEUQ TQEEE UIQQE EIUIE EUUUQ QIIUT

It? IIIET UEIQQ IQIQI EETEU ITIQQ QIIEI IIQTQ IQTEI EIQQE UTEIU

Hot QQUTQ TQIUI QQIIU UQTEI ETUUU UQTEI EEEIQ TEEQE QQTEU QIEEU

Diggety! QQQIE EUEIE IIIIQ TQQEU QTEUU QUEEU EIEEI EUQIU IEIIE EUIQI

QQIIT EIEET IUQQU TQTUE EEEIQ TQIIE IIQEI EEUEE UIUEE UQETI

Of course, if the letters are not in regular oder in the squares, then it is a bit harder, but at most it is not harder than any ordinary single-mixed alphabet cipher. One simple way of mixing up the order of the letters in the square is to use a key-word, and I'll show an example just by way of illustration.

You'll note in Figure 23 that the set of letters at the side and the set at the top are different in this case, so that the cipher message would here be composed of ten different letters.

	S	T	O	N	E
B	W	A	S	H	IJ
L	N	G	T	O	B
A	C	D	E	F	K
C	L	M	P	Q	R
K	U	V	X	Y	Z

Figure 23

The next problem is one based on this principle. If you'll use your ingenuity you can reconstruct, that is, build up the original cipher square as you dig into the cryptogram, and this will make the solution easier and more interesting. Try your hand at it and I warrant you'll do it.

PROBLEM 20

AAARC KARAA AAWAT MAKWK HMTAH MAMAA WKART KARAK AATRC RTMHM

TEARC RWRAR AAWEA RTEAR TMWKA RARTM WKAEW KTRCE ARTMH MCKAM

AAWKA EARAA TRCMW KWAHM TMWMA RTMCA WATMA KWEAR WKWKT KARCR ARTMW

KHMCK CMTKT RWACR WEWRT AAAAR CKARA AARAR WATMW RTRTM CEAAA

MWMWK CMTAW MAAHM CMARA RCAWA TMAKW EHMTM CAARC MARCR WRARA

AWKHK ARTKC KWKAE

There are other variations of this kind of cipher making use of a square, and they can become very hard depending on how many messages you have, the size of the diagram, and the arrangement of letters in the diagram. For example, it is possible to get up a diagram which will allow you to have 26 different pairs of equivalents for each letter of the alphabet, or you can arrange it so that the high-frequency letters like E, T, R, and so on have many more pairs to represent them than the low-frequency letters. But then those problems become too difficult for you at this sate of the game, so I'll omit them. The famous British Army cipher of pre-World War days, the Playfair, utilized a square, according to a special method.

That business of having certain English letters, the high-frequency ones especially, represented by more than one letter in the cryptogram is an old stunt. It was very popular in Poe's time. For example, here's a cipher alphabet based upon a phrase with the repeated letters in the phrase left in, so that certain cipher letters represent several plain-text letters.

English - A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Cipher - G O V E R N M E N T O F T H E U N I T E D S T A T E

Here the letter E_c can represent D_p, H_p, O_p, T_p, and Z_p. The one who receives the message must use his intelligence!

This old stunt was some years ago brought back to life in a mystery story by one of our most popular writers. If you think you'd like to tackle a cipher based on that scheme try Problem 21. I give it in two forms. In Problem 21 the text is in the regular five-letter group form. I think you will find it pretty tough, so if, after spending some time on it you don't get anywhere, tackle Problem 22, which is the same, except the original word lengths are shown. BUT DON'T TURN THE PAGE UNTIL YOU HAVE TRIED YOUR LEVEL BEST ON THE FIRST FORM, PROBLEM 21. DON'T CHEAT!

PROBLEM 21

Is WSTEL TESIE ARGSW SEPSL HSKIK GSSLI ASSET UITSO GEEGE OGEPR SAGSW

This SRSKU IEASC HTSKI PGSES FILSK GWIPR SGKES KNKSR SITSA PRSHK STTSL

A SPRIP TIUTS FSKSP RSSCH TSKSK SERSE SKSPS FSTTS ELSEE SKSIS NGEOP

Wow? RSSSA ESSPG SESAG AIEUH IKPSF PRSES ETUAG SWSRS KSATI EASTS TSEOP

SPRSL IGETI EASFI SGIWS ETAPR SSPKI GPTSF SEEAP RIPES ETATS IAPRS

RSUIO SKPRK SEORP RSGST IEAOK SEHSG EPSPR SGEAG IESWS IEIEA RSEFI

KAGSP IEPES KSPRS SRSKS SSFGE AGI

PROBLEM 22

WSTELTES IEA RGS WSEPSLHSKIKGSS LIAS SETU I TSOGEEGEO GE PRS AGSWSRSKU IEA SCHTSKIPGSE SF ILSKGWI PRSGK ESKN KSRSITSA PRS HKSTTSLS PRIP TIU TSFSKS PRS SCHTSKSKS ERS ESKS PS FSTTSE LSE ESKS IENGEO PRSSS AESSPGSES AGA IEU HIKP SF PRS ESETU AGSWSRSKSA TIEAS TSTSEO PS PRS LIGETIEA SF ISGI WSETA PRS SPKIGP TS FSEEA PRIP ESETA TSIA PRS RSUIOSK PRKSEOR PRS GSTIEA OKSEHS GEPS PRS GEAGIE SWSIE IEA RSE FIK AGSPIEP ESKS PRS SRSKSS SF GEAGI

Confusion Worse Confounded

The reason why ciphers based on alphabets like the one I've shown and taken from Poe are not used for serious work is that they are very slow and likely to lead to confusion in deciphering. For example, in one example I cameacross a case where I_c stood for E_p, J_p, R_p, T_p, and W_p; T_c stood for C_p, H_p, N_p, and D_p. The cipher word ITIII, therefore, deciphers as follows:

I	T	I	I	I
E	C	E	E	E
J	H	J	J	J
R	N	R	R	R
T	D	T	T	T
W		W	W	W

The plain-text can be any one of three words, THERE, THREE, and WHERE. It takes an inexperienced person much time to figure the message out even if he has the key. I should also have told you that ciphers in which two letters or two figures stand for a single letter of the English text are not popular for serious work either, because the cryptograms are twice as long as the original, and hence the cost of telegraphing them is twice as much as it should be. That's a reason that hits the business man right where he lives, and in these days of economy, everybody feels just the same way about it. No, they're not used if they can in any way be avoided.

CHAPTER VI.

A Horse Of Another Color. But Still A Horse.

Now for some figure ciphers - that is, cryptograms composed of numbers.

With the numbers from 1 to 100, you can get up four complete alphabets, if you make the letter I stand also for J. And you can use a key-word too. For example, here is one such set of alphabets based on the key-word, "CODE", that is, the first set begins with OI = C; the next, with 26 = O, and so on.

01 - C	26 - O	51 - D	76 - E
02 - D	27 - P	52 - E	77 - F
03 - E	28 - Q	53 - F	78 - G
04 - F	29 - R	54 - G	79 - H
05 - G	30 - S	55 - H	80 - IJ
06 - H	31 - T	56 - IJ	81 - K
07 - IJ	32 - U	57 - K	82 - L
08 - K	33 - V	58 - L	83 - M
09 - L	34 - W	59 - M	84 - N
10 - M	35 - X	60 - N	85 - O
11 - N	36 - Y	61 - O	86 - P
12 - O	37 - Z	62 - P	87 - Q
13 - P	28 - A	63 - Q	88 - R
14 - Q	39 - B	64 - R	89 - S
15 - R	40 - C	65 - S	90 - T
16 - S	41 - D	66 - T	91 - U
17 - T	42 - E	67 - U	92 - V
18 - U	43 - F	68 - V	93 - W
19 - V	44 - G	39 - W	94 - X
20 - W	45 - H	70 - X	95 - Y
21 - X	46 - IJ	71 - Y	96 - Z
22 - Y	47 - K	72 - Z	97 - A
23 - Z	48 - L	73 - A	98 - B
24 - A	49 - M	74 - B	99 - C
25 - B	50 - N	75 - C	00 - D

Using such a set of alphabets, each letter can have four different equivalents, so that repetitions can be hidden pretty effectively. For example, with the alphabets above, the word "ARRIVED" can be written in many different ways, among which are the followings

A	R	R	I	V	E	D
24-	64-	88-	46-	92-	03-	02, or
24-	15-	64-	56-	19-	76-	51, or
73-	88-	15-	07-	19-	52-	41, etc., etc.

Figures Can Be Used For Other Purposes Than Statistics

To make it look even more mysterious, you can run the figures together in groups of five. Like this:

24648 84692 0302.... etc.

How would you solve such a cipher?

Well, if it comes to you in groups of five figures, the first thing to do, of course, is to break it up into pairs. Then make your frequency tables. There will be four tables, because the numbers from 01 to 25 form one table; those from 26 to 50, the second table, and so on. If the message is fairly long, the number which stands for E will be apparent from its high frequency. Once you can locate E in each table the rest of the numbers merely follow the alphabet in its normal order. For example, in the illustration above, if you have found that 03 is the most frequent in the first tabulation - that is, from 01 to 25 - then you could assume that 03 = E_p. It would follow that 04 = F, 05 = G, and so on. Your points of high and low frequency should fall in the proper places to match the normal frequencies of English letters. To show you exactly what I mean, suppose you had a frequency table like this one at the right. You would assume that 03 = E; then 04 = F;

05 = G; 06 = H; and 07 = I.

Now you remember that I is a letter of high frequency, and the fact that 07 is of high frequency in this particular table is good evidence that you are on the right trail. But continue with it. 08 = K; 09 = L; 10 = M; 11 = N; and 12 = O. Here again you get more good evidence. K is a letter of very low frequency and 08 (=K) is absent; N and O are letters of high frequency in English, and your table shows high spots at those two points. On the other hand, 13 = P, and 14 = Q, both low spots is just as good evidence that you are on the right track because these are usually letters of low frequency. And so on. In other words, your high spots and your low spots must fall in the right places - and all that depends upon choosing the correct starting point. If you don't choose the correct starting point, then your table won't fit very well, that is, the high spots in the table will mark letters of normally low frequency, and vice versa. For example, suppose you choose 24 = E as a starting point. Then 25 = F. That's all right, for F is a low frequency letter. 01 = G; that's also all right. 02 = H; only fair, for H is a medium in frequency. 03 = I; its frequency is really too high, but we'll let it pass. 04 = K, which is all right. 05 = L, also all right. 06 = M, which is good, 07 = N, which is very good. But then 08 = O_p, normally

Haven't We Met Before?

Figue 24

a letter of very high frequency, and the table shows no occurrences of 08. That's bad. If you go through the rest of the sequence you'll find that 13 = T, and since 13 did not occure in the message, the "fit" there is very bad. 17 = X;-much too much. No, the "fit" as a whole, when you choose 24 equals E as a starting point, is very bad. But if you start with 03 = E, the "fit" is excellent.

Who
Was
It
Said
Success
Was
Perspiration
Arrived
At
Its
Goal?

When there are four tables, you just have to do this "fitting" four times, and then try it out on the message. If you've done the work correctly, the result will be the solution. Try this one:

PROBLEM 23

54348 02923 91427 00630 53933 52440 73232 40278 39592 24785
25263 49178 19323 91207 53238 38732 97028 72131 11543 41573
30519 13823 21350 65335 30592 67830 99258 34739 66218 90290
91341 24704 51642 79510 91223 50688 85013 07935 43064 05735
00361 18734 22276 64047 51044 56235 13532 22390 40941 35812
73263 93581 12940 40011 59129 40258 38230 58710 96198 83291
21540 59819 53222 33880 01704 50574 93295 92091 40807 01094
19822 33200 39801 22970 20474 08032 91000

There's a way to make this system much harder, and as usual it consists in mixing up the order of the letters in the alphabet. Look at these alphabets, based upon the word STENOGRAPHY, with the letters of the key word MAKE as the starting points in them:

01 - M	26 - A	51 - K	76 - E
02 - Q	27 - P	52 - L	77 - N
03 - U	28 - H	53 - M	78 - O
04 - V	29 - Y	54 - Q	79 - G
05 - W	30 - B	55 - U	80 - R
06 - X	31 - C	56 - V	81 - A
07 - Z	32 - D	57 - W	82 - P
08 - S	33 - F	58 - X	83 - H
09 - T	34 - I-J	59 - Z	84 - Y
10 - E	35 - K	60 - S	85 - B
11 - N	36 - L	61 - T	86 - C
12 - O	37 - M	62 - E	87 - D
13 - G	38 - Q	63 - N	88 - F
14 - R	39 - U	64 - O	89 - I-J
15 - A	40 - V	65 - G	90 - K
16 - P	41 - W	66 - R	91 - L
17 - H	42 - X	67 - A	92 - M
18 - Y	43 - Z	68 - P	93 - Q
19 - B	44 - S	69 - H	94 - U
20 - C	45 - T	70 - Y	95 - V
21 - D	46 - E	71 - B	96 - W
22 - F	47 - N	72 - C	97 - X
23 - I-J	48 - O	73 - D	98 - Z
24 - K	49 - G	74 - F	99 - S
25 - L	50 - R	75 - I-J	00 - T

Now you would have a good time trying to solve a short mesage based on this principle, because you have here a system using four mixed alphabets, letters from each alphabet being taken at random. But if the message is fairly long, there's hope. And you'll need to learn a valuable little trick which I'll call "matching alphabets" instead of using a longer and more scientific name. It will be best to use an example. Suppose you have a message starting off like this:

88123 05278 41891 113...

And the frequency tables for the whole message are as follows:

If
You
Must
Be
Highbrow
Call
It
Indirect
Symmetry

Figure 25

TABLE 1

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

TABLE 2

26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50

TABLE 3

51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75

TABLE 4

76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 00

Now suppose we try to match Tables 1 and 2, that is, put them together so that their spots correspond, as well as their low spots. For example, notice in Figure 25 that the region from 08 to 15 in Table 1 has several high spots and so does the region from 44 to 50 in Table 2. Let us put them side by side, shifting Table 2 so as to make these high spots coincide. Thus:

Figure 26

TABLE 1

Go																								
Easy																								
Now!	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

TABLE 2

	37	38	39	40	41	42	43	44	45	46	47	48	49	50	26	27	28	29	30	31	32	33	34	35	36

The high and low spots coincide so well that you would be justified in combining the two tables into one. And then you could add Tables 3 and 4 to them (shifting them, of course, to make their high and low spots coincide with those of Tables 1 and 2). The final result is that you have a single table with enough frequencies in it to solve the problems easily. That's the purpose of combining the individual tables - to get enough material to solve the single mixed alphabet that results. For example, combing the four alphabets above into one table we have the following:

Figure 27

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
37 38 39 40 41 42 43 44 45 46 47 48 49 50 26 27 28 29 30 31 32 33 34 35 36
53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 51 52
92 93 94 95 96 97 98 99 00 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91

You can make a trigraphic frequency table now and go ahead on the same basis of solving as the simple type of mixed alphabet substitution. It would be easier to substitute single letters; thus 01, 37, 53, and 92 might all be represented by A; 02, 38, 54 and 93 by B, and so on, in order to compile the trigraphic frequency table, and anyhow it would make it look simpler.

Do you think you'd like to try one of these?

PROBLEM 24

Looks
Like
A
Tough
Proposition

87185 46329 13857 10763 02007 91342 33376 79212 13699 71630
71891 15136 25027 56100 13752 99077 17137 00860 40757 73713
49873 88973 02657 11769 87291 86813 40677 77218 80631 53738
49859 71265 13534 16507 13406 76476 11867 93360 76487 57191
18679 06067 06517 62010 97790 98405 38953 39712 69474 10964
77175 39377 45861 64989 06932 67691 40937 74505 97149 70571
37951 34002 74840 19753 51826 49613 89411 09413 89290 56096
13790 20045 85337 94008 64842 57112 75774 29716 68136 39304
71851 46766

The last step in making this particular type of cipher complicated lies in drawing up four altogether different alphabets and using the numbers from 01 to 100 to represent the letters. But I won't give you a problem to solve because it would be too difficult for you unless I made it a very long message or else gave you a number of them all in the same key. You see, it is not possible in such a case to combine any of the alphabets, or rather frequency tables, because they are wholly independent of one another.

Warning!

But don't get the idea that a cipher of that type is getting toward the last word in secrecy. It's a very simple kind after all; there are systems in existence hundreds of times more difficult to solve.

What, More Numeral Ciphers?

Another common method of making up a cipher alphabet employing figures is shown at the left. Each letter of the alphabet can be represented by three different numbers. For example, A can be represented by 11, 21, 31; B by 12, 22, 32, and so on.

	1	2	3	4	5	6	7	8	9	0
1-2-3	A	B	C	D	E	F	G	H	I	J
4-5-6	K	L	M	N	O	P	Q	R	S	T
7-8-9	U	V	W	X	Y	Z	.	,	?	;

A cryptogram written by means of this particular cipher diagram would be pretty easy to solve once you knew the scheme because, as you see, the second figure in each group is the same for all three equivalents for any letter, and morever the order of the letters in the diagram is same as that in the ordinary alphabet, and the order of the figures is also normal. So, starting off with 11 = A, 12 = B, 13 = C, and so on, the cipher alphabet is not changed to amount to anything, and a cryptogram written by this means would be the simples kind of a thing.

But you can make lots of variations in the arrangement of either

the letters, or the figures, or both. Take a look at this one, for example. Here the second digit in the three pairs representing each letter is the same but the relation between the first digits in these pairs is broken up - they do not follow each other in sequence as was the case above, where A was 11, 21, 31; B 12, 22, 32, and so on. Furthermore, the alphabet is mixed. But phooey, that's nothing to you by now. You're just eating 'em up.

	7	2	9	1	8	4	0	3	5	6
6-3-8	W	O	R	K	I	N	G	D	A	Y
9-5-1	B	C	E	F	H	J	L	M	P	Q
2-7-4	S	T	U	V	X	Z				

The next problem is one of this type.

PROBLEM 25

89471 84954 77595 68516 51865 58689 41829 67770 47158 28552

29778 17040 87178 85881 59795 74758 17558 99026 80541 05850

41714 75829 65565 02744 26544 08225 41454 71327 50215 76545

22415 08777 28515 54048 17512 55922 78178 87785 40215 48476

56781 85085 82168 12952 86552 88974 87265 07174 59142 25826

15758 21617 74519 67781 40962 15576 17401 45218 86857 77450

25705 74710 40568 45451 27885 68546 26784 85228 88825 62581

76162 68085 29731 72759

So there you are. Bravo!

I have shown you only a few of the thousands of minor variations and changes that can be rung on this type of simple substitution cipher, but I think you understand the game now.

Speaking of numeral ciphers, there's the famous one used by the Russian Nihilists. It looks like this:

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

I Will The Last Word

The letter A is represented by 11, B by 12, M by 32, S by 43, Y by 54; the entire alphabet sequence of equivalents being

A	B	C	D	E	F	G	H	I-J	K	L	M	N
11	12	13	14	15	21	22	23	24	25	31	32	33

O	P	Q	R	S	T	U	V	W	X	Y	Z
34	35	41	42	43	44	45	51	52	53	54	55

This is merely another variation of the single alphabet cipher, you see, and a snap to solve, you say. Exactly. But the Nihilists had a way of complicating matters which was like this: Take a key-word and write down the numeral equivalents for the letters of the key-word; add these numerals to the numerical equivalents for the letters of your message; and lo! you have not a single-alphabet cipher message, but a 3 - 4 - 5 - 6.... cipher message of whatever the number of letters in your key-word. For example, if you enciphered the message "The King is dead, long live the King", here is how it would look (a) when enciphered direct from the numeral square, and (b) when the use of the key word C Z A R (13-55-11-42) makes an additional step that of adding 13-55-11-42 repetitively to the original numbers.

	T	H	E	K	I	N	G	I	S	D	E	A	D	L
(a)	44	23	15	25	24	33	22	24	43	14	75	11	14	31
(b)	57	78	26	67	37	88	33	66	56	69	26	53	27	86

	O	N	G	L	I	V	E	T	H	E	K	I	N	G
(a)	34	33	22	31	24	51	15	55	23	15	25	24	33	22
(b)	45	75	35	86	35	93	28	99	34	57	38	69	44	64

T H E K I N G I S D E A D L
(b) 57-78-26-67-37-88-33-66-56-69-26-53-27-86

O N G L I V E T H E K I N G
45-75-35-86-35-93-28-99-34-57-38-69-44-64

Note that in (a) you have a long repetition 44-23-15-25-24-33-22, which represent THE KING, but (b) the letters THE KING are represented first by 57-78-26-67-37-88-33, and the second time by 99-34-57-38-69-44-64. Note that there is only one repetition in (b) namely, 57. But it happens it is not an actual repetition at all; it represents the letter T in the first case and A in the second. Looks like a pretty nifty scheme, doesn't it? But figure it out. Just what does it mean?

Let's Close With An Anecdote

Now in 1896 or thereabouts, there appeared in the Pall Mall Magazine of London, a series of four articles on the subject of cryptography. The old pages were unearthed by a friend of mine last year in some dusty files. The writer described various cipher systems used since the beginning of history, and worked up to a description of the Nihilist cipher, his piece de resistance. He gave an example, using the key-word TYRANT (How many alphabets, therefore, did his message have?). Then at the end of his article he gave a very short cipher message without naming the key-word used to encipher it, and said: "And now the secret will remain forever hidden, for the lock has snapped shut and can never be unlocked". Quite a challenge, yes? Here is his message: 36-49-77-65-45-43-30-24-76-88-66-54-46-26-44-65-59-57-72-36. Well, when my husband, who I veritably believe is the smartest man that ever lived, met up with that message, he took the challenge and set his teeth into the tough nut with a snap; and would you believe it, he deciphered the message, short as it was, and the key, in 15 minutes! Of course when I learned that I too

had to try my hand it; with the result that I unlocked the forever-to-be-hidden secret in 17 minutes. (Does this make him a wife-beater?)

Why not take a try at this tough nut yourself? It's not too impossible. If you don't succeed now, come back to it after you've successfully completed all the rest in the book.